The use of video recordings by private individuals – a data protection analysis

03.04.2019

Following a recent Federal Supreme Court decision (Decision Federal Supreme Court 6B_181/2018 of 20 December 2018), the topic of CCTV-systems operated by private individuals has returned to the public spotlight. Not only do questions relate to the requirements to legally setting up and using CCTV-systems, but they also address the handling of the data obtained by these systems.

In particular: Are private persons obliged to hand over CCTV-data to the police, or to other law enforcement authorities, or even to their insurance company? What about the data protection and personality rights of the persons appearing on footage? And what are the regulations regarding storage and deletion of this data?

Because a constant recording of premises goes hand in hand with a constant processing of personal data, the risk arises of a potential violation of personal rights. Consequently, if you wish to install a CCTV-system around your office, shop or any other premises in Switzerland, you are not only subject to the Federal Act on Data Protection (the "FADP"), but you must also comply with the fundamental rights and freedoms provided for in the Federal Constitution (Art. 13 Federal Constitution). Under certain circumstances, further regulations contained in the Swiss Criminal Code (the "SCC") will apply.

Pestalozzi Rechtsanwälte AG
Feldeggstrasse 4
CH-8008 Zürich
T +41 44 217 91 11
zrh@pestalozzilaw.com

Pestalozzi Avocats SA
Cours de Rive 13
CH-1204 Genève
T +41 22 999 96 00
gva@pestalozzilaw.com

pestalozzilaw.com

1. Requirements to install and use a CCTV-system

First of all, it is important to note that public areas are generally subject to the monopoly of the state. Thus, private persons are not free to monitor just any random area. Hence, it must be distinguished which area is being surveilled: Are solely private premises affected or are public areas such as footpaths, entrance areas, public car parks, streets, etc. affected as well? Surveillance by private persons of purely or predominantly public areas is generally forbidden. If the extent of this intrusion, however, is negligible, and monitoring the private property would otherwise be impossible, common sense generally allows surveillance activities provided, however, that the relevant requirements as set out below are met. Alternative monitoring option would require the permission from the competent cantonal authorities.

As a first and most important prerequisite, a private person using CCTV-systems must ensure that it is evident for the individuals being recorded that they are in fact being recorded and that the personal data obtained are only processed for the purpose indicated at the time of the recording collection (Art. 4 FADP). That is, in general, any recorded person must be informed about the purpose, the type and the extent of the surveillance, as well as about the use of the data collected. Such purpose can, however, follow from the circumstances (e.g., obvious shop surveillance camera to prevent thefts).

Further, to be allowed to install a CCTV-system on private premises, one must meet the principles of legality and proportionality:

The principle of legality is met if (i) the affected person (e.g., a customer) consents to being recorded and so accepts the interference with his/her personality rights, (ii) there is a predominant public or (iii) private interest or (iv) if the recordings are justified by law (FDPIC-guidelines on video surveillance by private individuals available at www.edoeb.admin.ch). Consent may be given implicitly, for example, if a customer is informed – e.g., based on a publicly displayed sign – before entering a restaurant that CCTV-systems are being used and then voluntarily enters the restaurant. Security concerns such as protection from damages of property, protection from theft, or monitoring of manufacturing processes are examples of legitimate purposes and overriding private interests. An inadmissible private interest would be pure economic interest (e.g., a webcam used as a marketing tool).

To fulfill the requirement of proportionality, the processed data must be (i) suitable to achieve the purpose pursued and (ii) only data must be processed that are required for that purpose. The requirement of suitability is met if the surveillance is specific to the purpose (e.g., to avoid theft of a certain product, only that product is being surveilled). The requirement of necessity is met if the measure is chosen that at least infringes upon the personality rights of the recorded individual. In practice, this means, for instance, that a store intending to prevent thefts must, as a preliminary and milder measure, secure its products by way of locks before installing a CCTV-system.

2. Storage and deletion of CCTV-data

Personal data, such as the images of individuals recorded by CCTV-systems, must be protected against unauthorized processing through both adequate technical and organizational measures. This includes, inter alia, measures that allow confidentiality to be kept or, in other words, that access to surveillance data is granted on a need-to-know basis only and that access is secured (e.g., by a password or a key to a separate room where the data are kept).

In order to comply with the necessity requirement, all CCTV-data shall be generally deleted within 24 hours.

3. Obligation to surrender CCTV-data?

Since data processed by a CCTV-system showing individuals is considered to be personal data, one may not freely disclose and hand-over such data without a previous legal assessment. First, a distinction must be made between private recipients and authorities:

Any private person may request information from the controllerof a data file as to whether data concerning them and only them is being processed (Art. 8 FADP). The individual has the right to be informed about the following aspects:

1. all available data concerning the data subject in the data file;
2. purpose of the data;
3. legal basis for processing (if applicable);
4. categories of personal data processed; and
5. other parties involved with the file and data recipients.

The data and the information about the processing activities must be provided within 30 days after receiving the formal, written information request. Generally, the data must be provided at no cost (Art. 8 para. 5 FADP). A request may, however, be denied if there are third party overriding interests, or if the data file controller argues he/she has own overriding interests.

By law, no private person has the right to request disclosure of CCTV-data from another private person. This right is neither available to insurance companies nor to private security companies. Thus, both the CCTV-systems' private operator and the data controller must always and, before disclosing any personal data to third parties carefully weigh the interests at stake. They must particularly consider the data subject's personal and data protection rights as well as the indicated purpose of the CCTV-system itself. Whether the purpose covers disclosure to certain third parties, whether disclosure is proportionate and which interests prevail can only be decided on a case by case basis, taking into account all circumstances.

The case is different if state authorities request disclosure of the recorded data. The disclosure of personal data to law enforcement authorities such as the police or the public prosecutor is only permitted if there is (i) a legal basis for it, (ii) an overriding private or (iii) public interest, or if (iv) the concerned data subject consents to it.

A sufficient legal basis is, for instance, a seizure order (Art. 263 Criminal Procedure Code). For that, a formal order ("Verfügung") issued by the public prosecutor's office or by a competent court is generally necessary. In certain circumstances, a temporary seizure order by the police without a written order may be considered as a sufficient legal basis (e.g., in case of imminent danger). This type of procedure should, however, remain the exception for obtaining CCTV-recordings.

A second possibility is the release of CCTV-data based on an overriding private or public interest. Whether this specific private or public interest is given, must be analyzed and established on a case by case basis, taking into account all interests at stake.

According to the Federal Supreme Court's recent decision mentioned above, the formalities are even stricter if the police intends to surveil private premises. In addition to the public prosecutor's office's formal order, the compulsory measures court must approve this order.

Without approval, no CCTV-system can be legally installed by the police on private premises, and if done nevertheless without authorization, the evidence obtained from such a system may not be used in court (e.g., to prove theft) (Decision Federal Supreme Court 6B_181/2018 of 20 December 2018, consid. 4.2). For all these reasons, even police enquiries should be judged critically, and CCTV-data and recordings should not be disclosed lightly. In contrast, if a CCTV-system is legally installed by private persons, the recordings may be used as evidence to support a civil or criminal claim.

4. Potential penalties for non-compliance

In case of non-compliance with the above mentioned principles, criminal liability may be faced. Noteworthy is the breach of secrecy or privacy through the use of an image-carrying device, according to art. 179quarter SCC. A person fulfilling the relevant requirements is liable – on complaint – to a custodial sentence not to exceed three years or to a monetary penalty up to CHF 540'000. Furthermore, personal data from recordings used, processed or disclosed in violation of data protection laws may not only have criminal consequences, but the infringer may also face a civil claim brought forward by the data subject.

In case of refusal to disclose CCTV-data required by an official order of a state authority (e.g., from the public prosecutor's office or from a competent court), a fine based on art. 292 SCC up to CHF 10'000 may be ordered.

5. Recommendations

If you intend to install a CCTV-system, you should first verify the following:

1. For which purpose is the CCTV-system intended?
2. What area shall be monitored (i.e., only private premises or also public areas)?
3. Is the CCTV-system an adequate and proportionate measure for the intended purpose, or are there ways to achieve the specific purpose that are less harmful to the privacy of individuals?

4. Is the consent of the surveilled person necessary (i.e., can people be identified based on the system's recordings)?

5. Are there overriding private or public interests for installing a CCTV-system (cue: security reasons vs. marketing)?

In case you receive a request for disclosure of CCTV-data and recordings, you should verify the following:

1. In case a private person is requesting disclosure:

- Is the private person identical with the data subject? If so, does a right to information based on art. 8 FADP exist? If not:
- Does the CCTV-systems' purpose cover the disclosure of personal data to the requesting private person? Is there an overriding interest to disclose the CCTV-data, or are the data subject's interests given priority?

2. In case a state authority is requesting disclosure:

- Is the request based on a formal written order by a competent state authority? If not, a written order must be requested first, before disclosing any data.
- If no formal order is provided, a written statement must be requested, explaining the kind of private or public interest the request is based on.

Contributors: Dr. Lorenza Ferrari Hofer (Partner), Janine Reudt-Demont (Senior Associate), Matthias Niklaus (Junior Associate)

Michèle Burnier

Partner
Attorney at law

Pestalozzi Attorneys at Law Ltd
Cours de Rive 13
1204 Geneva
Switzerland
T +41 22 999 96 00
michele.burnier@pestalozzilaw.com